PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro
INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 7 : E05B 49/00 — A2

(11) Internationale Veröffentlichungsnummer: WO 00/14369

(43) Internationales Veröffentlichungsdatum: 16. März 2000 (16.03.00)

(21) Internationales Aktenzeichen: PCT/DE99/02811

(22) Internationales Anmeldedatum: 4. September 1999 (04.09.99)

(30) Prioritätsdaten:
PP 5763 — 9. September 1998 (09.09.98) — AU
43414/99 — 5. August 1999 (05.08.99) — AU

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: ROBERT BOSCH GMBH [DE/DE]; Postfach 30 02 20, D–70442 Stuttgart (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: STROHBECK, Walter [DE/AU]; 11 Mack Road, Narre Warren 3805 (AU).

(81) Bestimmungsstaaten: BR, JP, KR, US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

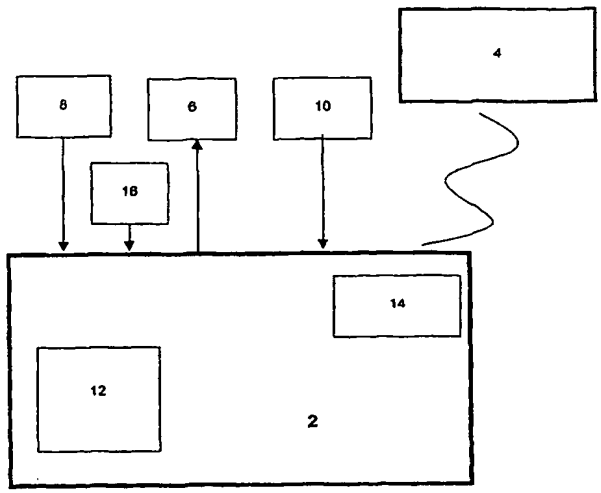
Veröffentlicht
Ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts.

(54) Title: METHOD FOR CONTROLLING A CODE

(54) Bezeichnung: EIN SCHLÜSSELKONTROLLVERFAHREN

(57) Abstract

The invention relates to a method for controlling a code in a security system and to a security system comprising at least one permissible code and electronic control means consisting of a transmitter/receiver for communication with at least one permissible code. The control means produce an authorization for access to a secure object when authentication data is received from the at least one permissible code and store determinate identification data for the at least one permissible code. The method includes access to determinate identification data for the at least one permissible code in a mode of said system. The inventive method is characterized in that enabling data, corresponding to the determinate identification data of the at least one permissible code, is stored and the user follows a predetermined procedure in order to enter into a code validation mode of said system, maintain the enabling data for permissible codes in said validation mode inside the range of the transmitter/receiver and to delete the enabling data for permissible codes located outside the range of the transmitter/receiver, whereby codes without enabling data for the system are deactivated.



(57) Zusammenfassung

Ein Schlüsselkontrollverfahren für ein Sicherheitssystem und Sicherheitssystem, welches mindestens einen zulässigen Schlüssel und elektronische Kontrollmittel mit einem Sender/Empfänger für die Kommunikation mit dem mindestens einen zulässigen Schlüssel aufweist, wobei die Kontrollmittel eine Befugnis für Zugang zu einem gesicherten Gegenstand erzeugen, wenn Authentifizierungsdaten von dem mindestens einen zulässigen Schlüssel empfangen werden und eindeutige Identifizierungsdaten für den mindestens einen zulässigen Schlüssel speichern, wobei das Verfahren den Zugang zu den eindeutigen Identifizierungsdaten für den mindestens einen zulässigen Schlüssel in einem Modus des Systems einschließt; dadurch charakterisiert, daß Freigabedaten gespeichert werden, die den eindeutigen Identifizierungsdaten des mindestens einen zulässigen Schlüssels entsprechen, wobei ein Benutzer ein vorherbestimmtes Verfahren befolgt, um in einen Schlüssel–validierungsmodus des Systems einzuspringen, und in dem Validierungsmodus die Freigabedaten für zulässige Schlüssel innerhalb des Bereichs des Sender/Empfängers festzuhalten und die Freigabedaten für zulässige Schlüssel, die sich außerhalb des Bereichs des Sender/Empfängers befinden, zu löschen, wobei Schlüssel ohne die Freigabedaten für das System deaktiviert werden.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	**ES**	Spanien	**LS**	Lesotho	**SI**	Slowenien
AM	Armenien	**FI**	Finnland	**LT**	Litauen	**SK**	Slowakei
AT	Österreich	**FR**	Frankreich	**LU**	Luxemburg	**SN**	Senegal
AU	Australien	**GA**	Gabun	**LV**	Lettland	**SZ**	Swasiland
AZ	Aserbaidschan	**GB**	Vereinigtes Königreich	**MC**	Monaco	**TD**	Tschad
BA	Bosnien-Herzegowina	**GE**	Georgien	**MD**	Republik Moldau	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagaskar	**TJ**	Tadschikistan
BE	Belgien	**GN**	Guinea	**MK**	Die ehemalige jugoslawische Republik Mazedonien	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Griechenland			**TR**	Türkei
BG	Bulgarien	**HU**	Ungarn	**ML**	Mali	**TT**	Trinidad und Tobago
BJ	Benin	**IE**	Irland	**MN**	Mongolei	**UA**	Ukraine
BR	Brasilien	**IL**	Israel	**MR**	Mauretanien	**UG**	Uganda
BY	Belarus	**IS**	Island	**MW**	Malawi	**US**	Vereinigte Staaten von Amerika
CA	Kanada	**IT**	Italien	**MX**	Mexiko		
CF	Zentralafrikanische Republik	**JP**	Japan	**NE**	Niger	**UZ**	Usbekistan
CG	Kongo	**KE**	Kenia	**NL**	Niederlande	**VN**	Vietnam
CH	Schweiz	**KG**	Kirgisistan	**NO**	Norwegen	**YU**	Jugoslawien
CI	Côte d'Ivoire	**KP**	Demokratische Volksrepublik Korea	**NZ**	Neuseeland	**ZW**	Zimbabwe
CM	Kamerun			**PL**	Polen		
CN	China	**KR**	Republik Korea	**PT**	Portugal		
CU	Kuba	**KZ**	Kasachstan	**RO**	Rumänien		
CZ	Tschechische Republik	**LC**	St. Lucia	**RU**	Russische Föderation		
DE	Deutschland	**LI**	Liechtenstein	**SD**	Sudan		
DK	Dänemark	**LK**	Sri Lanka	**SE**	Schweden		
EE	Estland	**LR**	Liberia	**SG**	Singapur		

EIN SCHLÜSSELKONTROLLVERFAHREN

Die vorliegende Erfindung bezieht sich auf ein Schlüsselkontrollverfahren und ein Sicherheitssystem.

Es sind passive Sicherheitssysteme für Fahrzeuge vorhanden, die fernbetätigte Schlüssel mit Transpondern verwenden, die mit einem Sender/Empfänger eines Fahrzeugs kommunizieren, wenn der Transponder innerhalb eines bestimmten Bereichs des Sender/Empfängers ist. Vorausgesetzt, daß die Kommunikation zwischen einem Schlüssel und dem Sender/Empfänger einem vorherbestimmten Kommunikationsprotokoll folgt, und eindeutige Authentifizierungsdaten ausgetauscht und für gültig erklärt werden, wird der Schlüssel als zulässiger Schlüssel erklärt und das System gewährt Einlaß und/oder Benutzung des Fahrzeugs. Wenn der zulässige Schlüssel sich in der Folge außerhalb des Bereichs des Sender/Empfängers bewegt, sichert das Sicherheitssystem das Fahrzeug durch Verschließen und Immobilisieren des Fahrzeugs.

Wenn ein zulässiger Schlüssel für ein Fahrzeug verloren geht, muß der Schlüssel deaktiviert werden, so daß er

nicht mehr dazu benutzt werden kann, Zugang zu dem Fahrzeug zu gewähren. Es ist daher wünschenswert, eine einfache Methode zur Deaktivierung verlorener Schlüssel und zur Reaktivierung wiedergefundener zulässiger Schlüssel zu finden, insbesondere wenn die Schlüssel nicht mit Druckknöpfen ausgerüstet sind.

Die vorliegende Erfindung stellt ein Schlüsselkontrollverfahren für ein Sicherheitssystem vor, welches mindestens einen zulässigen Schlüssel und elektronische Kontrollmittel mit einem Sender/Empfänger für die Kommunikation mit dem mindestens einen zulässigen Schlüssel aufweist, wobei die Kontrollmittel eine Befugnis für Zugang zu einem gesicherten Gegenstand erzeugen, wenn Authentifizierungsdaten von dem mindestens einen zulässigen Schlüssel empfangen werden und eindeutige Identifizierungsdaten für den mindestens einen zulässigen Schlüssel speichern, wobei das Verfahren den Zugang zu den eindeutigen Identifizierungsdaten für den mindestens einen zulässigen Schlüssel in einem Modus des Systems einschließt;
dadurch charakterisiert, daß Freigabedaten gespeichert werden, die den eindeutigen Identifizierungsdaten des mindestens einen zulässigen Schlüssels entsprechen, wobei ein Benutzer ein vorherbestimmtes Verfahren befolgt, um in einen Schlüsselvalidierungsmodus des Systems einzuspringen, und in dem Validierungsmodus die Freigabedaten für zulässige Schlüssel innerhalb des Bereichs des Sender/Empfängers festzuhalten und die

Freigabedaten für zulässige Schlüssel, die sich außerhalb des Bereichs des Sender/Empfängers befinden, zu löschen, wobei Schlüssel ohne die Freigabedaten für das System deaktiviert werden.

Die vorliegende Erfindung stellt auch ein Sicherheitssystem vor, welches mindestens einen zulässigen Schlüssel und elektronische Kontrollmittel mit einem Sender/Empfänger für die Kommunikation mit dem mindestens einen zulässigen Schlüssel aufweist, wobei die Kontrollmittel eine Befugnis für Zugang zu einem gesicherten Gegenstand erzeugen, wenn Authentifizierungsdaten von dem mindestens einen zulässigen Schlüssel empfangen werden, und eindeutige Identifizierungsdaten für den mindestens einen zulässigen Schlüssel speichern, wobei das Verfahren einen Modus für den Zugang zu den eindeutigen Identifizierungsdaten für den mindestens einen zulässigen Schlüssel aufweist;

dadurch charakterisiert, daß die Kontrollmittel Freigabedaten entsprechend den eindeutigen Identifizierungsdaten für den mindestens einen zulässigen Schlüssel speichern, wenn sie für das System aktiviert werden, und daß die Kontrollmittel

in einen Schlüsselvalidierungsmodus einspringen, wenn ein Benutzer ein vorherbestimmtes Verfahren befolgt, und in dem Validierungsmodus Freigabedaten für zulässige Schlüssel innerhalb des Bereichs des

Sender/Empfängers festgehalten und für zulässige Schlüssel außerhalb des Bereichs des Sender/Empfängers gelöscht werden.

Eine bevorzugte Realisierung der vorliegenden Erfindung ist anschließend mit Bezug auf die beiliegende Zeichnung als Beispiel beschrieben, wobei:

Figur 1 ein Blockdiagramm einer bevorzugten Realisierung eines Sicherheitssystems ist;

Ein Sicherheitssystem, wie in Figur 1 gezeigt, schließt folgende ein:
eine elektronische Kontrolleinheit (ECU) 2, welche in ein Fahrzeug eingebaut ist und eine Verarbeitungsschaltung zur Kommunikation mit anderen elektrischen und elektronischen Teilen des Fahrzeugs und des Sicherheitssystems aufweist. Insbesondere beinhaltet die ECU 2 einen RF-Sender/Empfänger 14 zur Erzeugung eines RF-Signals, welches den Transponder eines fernbetätigten Schlüssels 4 des Sicherheitssystems erregt, wenn der Schlüssel 4 sich in der Nähe eines Fahrzeugs befindet.
Der Schlüssel 4 kann eine Karte oder einen "Fob" enthalten. Wenn er einmal erregt ist, benutzt der Schlüssel 4 RF-Übertragungsverfahren, um mit dem Sender/Empfänger gemäß einem sicheren Kommunikationsprotokoll zu kommunizieren, um Authentifizierungsdaten von dem Schlüssel 4 zu der ECU 2 weiterzuleiten. Wenn diese empfangen worden sind,

vergleicht die ECU 2 die Authentifizierungsdaten mit Sicherheitsdaten in ihrem Speicher, nämlich Sicherheitscodes und Freigabemarken, die in einem EEPROM 12 (elektrisch löschbarer programmierbarer Festwertspeicher) gespeichert sind. Wenn die ECU 2 eine Übereinstimmung zwischen den empfangenen Authentifizierungsdaten und ihren eigenen Sicherheitsdaten findet, gibt die ECU 2 Signale an die anderen Teile des Fahrzeugs ab, Zugang zu dem Fahrzeug oder Inbetriebnahme des Fahrzeugs für den Besitzer des Schlüssels 4 zu ermöglichen. Wenn der Schlüssel 4 aus der unmittelbaren Nähe des Fahrzeugs entfernt wird, wird dies von dem Sender/Empfänger 14 erkannt, welcher dann die ECU 2 veranlaßt, Signale zu erzeugen, um das Fahrzeug zu sichern, zum Beispiel durch Verschließen und Immobilisieren des Fahrzeugs.

Normalerweise kann bei Sicherheitssystemen eine Anzahl zulässiger Schlüssel benutzt werden, um Zugang zu dem Fahrzeug zu erlangen. Die Schlüssel 4 schließen jeweils eine eindeutige Serien- oder Identifizierungsnummer ein, und diese wird der ECU 2 als Bestandteil der Authentifizierungsdaten kommuniziert. Die ECU 2 speichert die Seriennummern für jeden zulässigen Schlüssel in ihrem EEPROM 12, und für jede Seriennummer ist eine Freigabemarke (enable flag) gespeichert. Als Alternative zu der Freigabemarke kann das System ein Kontrollbyte speichern, bei welchem es sich um eine verschlüsselte Version der Identifizierungsnummer handeln kann. Während des Authentifizierungsverfahrens,

wenn die ECU 2 die Authentifizierungsdaten überprüft, prüft der ECU 2 um zu ermitteln ob die empfangene Seriennummer des kommunizierenden Schlüssels 4 in dem EEPROM 12 gespeichert ist und ob die Freigabemarke eingestellt oder zurückgestellt ist. Falls die Seriennummer gefunden wird und die Freigabemarke eingestellt ist, dann ist der kommunizierende Schlüssel ein zulässiger Schlüssel, welcher dazu benutzt werden kann, Zugang zu dem Fahrzeug zu erlangen. Falls jedoch die Seriennummer gefunden wird und die Freigabemarke nicht eingestellt ist, dann ist der kommunizierende Schlüssel nicht mehr ein zulässiger Schlüssel, der benutzt werden kann. Die ECU 2 ist in der Lage, eine Deaktivierung des Schlüssels und ein Aktivierungsverfahren durchzuführen, welche die Freigabemarke für Schlüssel 4 zurückstellt und einstellt. Dies ermöglicht einem Fahrzeugbesitzer mit verlorenen oder gestohlenen Schlüsseln auf eine einfache Art und Weise, so wie vorstehend beschrieben, zu verfahren.

Wenn ein zulässiger Schlüssel verloren oder gestohlen wurde, kann der Besitzer von mindestens einem verbleibenden zulässigen Schlüssel die ECU 2 in einen Schlüsselvalidierungsmodus versetzen, um alle die restlichen Schlüssel zu validieren. Der Besitzer der restlichen Schlüssel steigt einfach in das Fahrzeug ein, und bringt alle die restlichen Schlüssel innerhalb den Bereich des Sender/Empfängers 14, und führt ein vorherbestimmtes Verfahren durch, die ECU 2 in den

Schlüsselvalidierungsmodus zu verbringen. Wenn die ECU 2 in Schlüsselvalidierungsmodus ist, schaltet die ECU 2 alle die in ihrem Bereich befindlichen Schlüssel 4 ein, um ihre Seriennummer zu empfangen, und stellt die Freigabemarken in dem EEPROM 12 für die empfangenen Seriennummern ein, während die Freigabemarken für sämtliche anderen in dem EEPROM 12 gespeicherten Schlüsselseriennummern zurückgestellt werden. Die Schlüssel, die sich daher innerhalb des Bereichs des Sender/Empfängers 14 befinden, werden dann zulässige Schlüssel darstellen, und der verlorene odeer gestohlene Schlüssel wird nicht mehr länger ein zulässiger Schlüssel sein, da seine Freigabemarke zurückgestellt ist. Vollendung des Schlüsselvalidierungsverfahrens wird von der ECU 2 angezeigt, die ein Abschlußsignal für eine Nachrichteneinheit 6 erzeugt. Die Nachrichteneinheit zeigt einfach entweder sichtbar oder hörbar an, daß das Schlüsselvalidierungsverfahren abgeschlossen ist. Die Nachrichteneinheit 6 kann eine Leuchtdiode in dem Fahrzeug oder aber die Hupe oder Sirene des Fahrzeugs sein. Die Nachrichteneinheit 6 kann auch eine Anzeigeeinheit in dem Fahrzeug sein, welche die Daten empfängt und in der Lage ist, anzuzeigen, welche Schlüssel für das Fahrzeug zulässig sind. Die Anzeigeeinheit würde auch andere Nachrichten anzeigen, wie z.B. "Schlüsselvalidierung abgeschlossen", und kann Kontrollen einschließen, welche einem Benutzr des Fahrzeugs ermöglichen, eine Anzeige abzurufen, welche

die zulässigen Schlüssel anzeigt, wie z.B. Schlüssel A, B und C.

Wenn der verlorene oder gestohlene Schlüssel 4 wiedererlangt wird, kann der Schlüssel revalidiert oder neu aktiviert werden, indem wiederum alle die Schlüssel ins Fahrzeug gebracht werden und die ECU2 in Schlüsselvalidierungsmodus gebracht wird, um das vorstehend aufgeführte Schlüsselvalidierungsverfahren durchzuführen. Die Freigabemarke für den gefundenen Schlüssel 4 wird dann in dem EEPROM 12 eingestellt.

Um die Notwendigkeit zusätzlicher Hardware-Teile in dem Fahrzeug zu vermeiden, muß das benutzte vorherbestimmte Verfahren, um die ECU 2 in den Schlüsselvalidierungsmodus zu versetzen, unter Verwendung schon vorhandener Fahrzeugteile durchgeführt werden. Das vorherbestimmte Verfahren sollte vorteilhafterweise die Verwendung von Teilen und Arbeitsgängen beinhalten, die normalerweise mit dem Starten oder dem Einlaß in das Fahrzeug verbunden sind. Die meisten Fahrzeuge haben eine Startmethode, bei welcher ein Pedal 8 betätigt werden muß, bei welchem es sich um das Brems- oder Kupplungspedal handelt, und dann gleichzeitig der Zündanlaßschalter 10 des Fahrzeugs betätigt werden muß. Die ECU 2 ist mit dem elektrischen Netzwerk oder Kabelbaum des Fahrzeugs verbunden, damit es die erzeugten Signale empfangen kann, wenn das Pedal 8 heruntergedrückt wird und der Zündanlaßschalter 10 betätigt wird. Zu dem

vorherbestimmten Verfahren zum Einspringen in den Schlüsselvalidierungsmodus kann dann hinzukommen, daß der Schlüsselbesitzer einfach abwechselnd mehrere Male das Pedal 8 herunterdrückt und den Zündschalter 8 betätigt, sagen wir dreimal, anstatt dies gleichzeitig zu tun. Wenn die ECU 2 die abwechselnde Betätigung des Pedals 8 und des Zündanlaßschalters 10 entdeckt, kann sie dann eine Nachricht für die Nachrichteneinheit 6 erzeugen, um den Einsprung in den Schlüsselvalidierungsmodus zu bestätigen, wenn das vorherbestimmte Verfahren durchgeführt worden ist. Die ECU 2 kann auch Aufrufe an die Nachrichteneinheit 6 erteilen, der Zeitsequenz für die Betätigung des Pedals 8 und des Zündanlaßschalters 8 zu folgen, um dem Schlüsselbesitzer bei der korrekten Durchführung des Verfahrens zur Eingabe des Schlüsselvalidierungsmodus behilflich zu sein. Alternativ können die Schritte und die Fahrzeugteile, die beim Einstieg in das Fahrzeug erforderlich sind, benutzt werden. In einigen passiven Sicherheitssystemen wird zum Beispiel der Schlüssel beim Anheben eines Türgriffes 16 erregt. Das vorherbestimmte Verfahren, das zur Eingabe des Schlüsselvalidierungsmodus erforderlich ist, könnte zum Beispiel beinhalten, daß ein Schlüsselbesitzer den Türgriff 16 mehrere Male innerhalb einer bestimmten Zeitspanne, z.B. viermal in zwei Sekunden, anhebt.

Die ECU 2 kann durch eine Anzahl von ECUs gestellt werden, oder in eine Anzahl von ECUs aufgeteilt werden, und ähnlich kann das Fahrzeug eine Anzahl von

Sender/Empfängern und Antennen zur Kommunikation mit fernbetätigten Schlüsseln 4 einschließen,. Die Schlüssel 4 können Schlüssel für passiven Zugang darstellen, die Energie seitens des Fahrzeugs erfordern, um mit der ECU 2 kommunizieren zu können, oder die Schlüssel können ihre eigene Batterieversorgung haben. Während die vorliegende Erfindung besonders vorteilhaft für Schlüssel ist, die keine Betätigungsknöpfe haben, können die Schlüssel 4 aber auch Betätigungsknöpfe aufweisen, und das Sicherheitssystem kann eine Kombination aktiver und passiver Sicherheitssysteme darstellen. Zum Beispiel kann das Sicherheitssystem so ausgelegt sein, daß der Schlüssel 4 bei Aktivierung in der Lage ist, über eine Entfernung, z.B. 30 m, mit dem Fahrzeug zu kommunizieren, und ist auch in der Lage, eingeschaltet oder erregt zu werden, wenn er sich näher am Fahrzeug befindet, wie z.B. durch Anheben des Türgriffes, oder durch irgendeine andere Betätigungseinrichtung, wenn er sich in der Nähe des Fahrzeugs befindet.

Dem Fachkundigen werden hierzu eine Vielzahl von Abwandlungen gegenwärtig werden, ohne daß der Umfang der vorliegenden Erfindung, wie sie hiermit unter Bezug auf die beiliegende Zeichnungen beschrieben wird, überschritten wird.

PATENTANSPRÜCHE

1. Ein Schlüsselkontrollverfahren für ein Sicherheitssystem, welches mindestens einen zulässigen Schlüssel und elektronische Kontrollmittel mit einem Sender/Empfänger für die Kommunikation mit dem mindestens einen zulässigen Schlüssel aufweist, wobei die Kontrollmittel eine Befugnis für Zugang zu einem gesicherten Gegenstand erzeugen, wenn Authentifizierungsdaten von dem mindestens einen zulässigen Schlüssel empfangen werden und eindeutige Identifizierungsdaten für den mindestens einen zulässigen Schlüssel speichern, wobei das Verfahren den Zugang zu den eindeutigen Identifizierungsdaten für den mindestens einen zulässigen Schlüssel in einem Modus des Systems einschließt;
dadurch charakterisiert, daß Freigabedaten gespeichert werden, die den eindeutigen Identifizierungsdaten des mindestens einen zulässigen Schlüssels entsprechen, wobei ein Benutzer ein vorherbestimmtes Verfahren befolgt, um in einen Schlüssel-validierungsmodus des Systems einzuspringen, und in dem Validierungsmodus die Freigabedaten für zulässige Schlüssel innerhalb des Bereichs des Sender/Empfängers festzuhalten und die Freigabedaten für zulässige Schlüssel, die sich außerhalb des Bereichs des Sender/Empfängers befinden, zu löschen, wobei Schlüssel ohne die Freigabedaten für das System deaktiviert werden.

2. Ein Schlüsselkontrollverfahren gemäß Anspruch 1, in welchem das vorherbestimmte Verfahren Schritte des Startverfahrens eines Fahrzeugs einschließt.

3. Ein Schlüsselkontrollverfahren gemäß Anspruch 1, in welchem das vorherbestimmte Verfahren Schritte eines Zugangsverfahrens in ein Fahrzeug einschließt.

4. Ein Schlüsselkontrollverfahren gemäß Anspruch 1, in welchem das vorherbestimmte Verfahren die Durchführung von Schritten unter Verwendung von Standardkontrollen eines Fahrzeugs einschließt.

5. Ein Schlüsselkontrollverfahren gemäß Anspruch 4, in welchem die Standardkontrollen ein Bremspedal, ein Kupplungspedal, einen Zündanlaßschalter, und/oder einen Türgriff einschließt.

6. Ein Schlüsselkontrollverfahren gemäß einem der Ansprüche 2 bis 5, in welchem die Schritte zu Zeitpunkten, relativ zu einander, durchgeführt werden, die sich von den Zeiten für die Standardverfahren für das Fahrzeug unterscheiden.

7. Ein Schlüsselkontrollverfahren gemäß einem der vorhergehenden Ansprüche, einschließlich Abschluß des Schlüsselvalidierungsmodus.

8. Ein Schlüsselkontrollverfahren gemäß Anspruch 7, in welchem die Anzeige die Erzeugung einer Anzeige der aktivierten zulässigen Schlüssel für das System einschließt.

9. Ein Schlüsselkontrollverfahren gemäß einem der vorhergehenden Ansprüche, in welchem die Schlüssel keine Betätigungsknöpfe aufweisen.

10. Ein Schlüsselkontrollverfahren gemäß einem der vorhergehenden Ansprüche, in welchem die Freigabedaten ein Kontrollbyte sind.

11. Ein Schlüsselkontrollverfahren gemäß einem der Ansprüche 1 bis 10, in welchem die Befugnis Zugang zu dem gesicherten Gegenstand gewährt.

12. Ein Schlüsselkontrollverfahren gemäß Anspruch 11, in welchem der gesicherte Gegenstand ein Fahrzeug ist.

13. Ein Schlüsselkontrollverfahren gemäß einem der Ansprüche 1 bis 10, in welchem der gesicherte Gegenstand ein Fahrzeug ist und die Befugnis die Inbetriebnahme des Fahrzeugs gewährt.

14. Ein Schlüsselkontrollverfahren gemäß Anspruch 13, in welchem die Inbetriebnahme das Starten des Fahrzeugs einschließt.

15. Ein Sicherheitssystem, welches mindestens einen zulässigen Schlüssel und elektronische Kontrollmittel mit einem Sender/Empfänger für die Kommunikation mit dem mindestens einen zulässigen Schlüssel aufweist, wobei die Kontrollmittel eine Befugnis für Zugang zu einem gesicherten Gegenstand erzeugen, wenn Authentifizierungsdaten von dem mindestens einen zulässigen Schlüssel empfangen werden, und eindeutige Identifizierungsdaten für den mindestens einen zulässigen Schlüssel speichern, wobei das Verfahren einen Modus für den Zugang zu den eindeutigen Identifizierungsdaten für den mindestens einen zulässigen

Schlüssel aufweist;
dadurch charakterisiert, daß die Kontrollmittel Freigabedaten entsprechend den eindeutigen Identifizierungsdaten für den mindestens einen zulässigen Schlüssel speichern, wenn sie für das System aktiviert werden, und daß die Kontrollmittel in einen Schlüsselvalidierungsmodus einspringen, wenn ein Benutzer ein vorherbestimmtes Verfahren befolgt, und in dem Validierungsmodus Freigabedaten für zulässige Schlüssel innerhalb des Bereichs des Sender/Empfängers festgehalten und für zulässige Schlüssel außerhalb des Bereichs des Sender/Empfängers gelöscht werden.

16. Ein Sicherheitssystem gemäß Anspruch 15, in welchem das vorherbestimmte Verfahren Schritte eines Startverfahrens eines Fahrzeugs einschließt.

17. Ein Sicherheitssystem gemäß Anspruch 15, in welchem das vorherbestimmte Verfahren Schritte eines Zugangsverfahrens in ein Fahrzeug einschließt.

18. Ein Sicherheitssystem gemäß Anspruch 15, in welchem das vorherbestimmte Verfahren die Durchführung von Schritten unter Verwendung von Standardkontrollen eines Fahrzeugs einschließt.

19. Ein Sicherheitssystem gemäß Anspruch 18, in welchem die Standardkontrollen ein Bremspedal, ein Kupplungspedal, einen Zündanlaßschalter, und/oder einen Türgriff einschließen.

20. Ein Sicherheitssystem gemäß einem der Ansprüche 16 bis 19, in welchem die Schritte zu Zeitpunkten, relativ zu

einander, durchgeführt werden, die sich von den Zeiten für die Standardverfahren für das Fahrzeug unterscheiden.

21. Ein Sicherheitssystem gemäß einem der Ansprüche 15 bis 20, einschließlich Mitteln zur Anzeige des Abschlusses des Schlüsselvalidierungsmodus.

22. Ein Sicherheitssystem gemäß Anspruch 21, in welchem die Anzeigemittel die Anzeige der aktuell zulässigen Schlüssel für das System einschließen.

23. Ein Sicherheitssystem gemäß einem der Ansprüche 15 bis 22, in welchem die Schlüssel keine Betätigungsknöpfe aufweisen.

24. Ein Sicherheitssystem gemäß einem der Ansprüche 15 bis 23, in welchem die Freigabedaten ein Kontrollbyte sind.

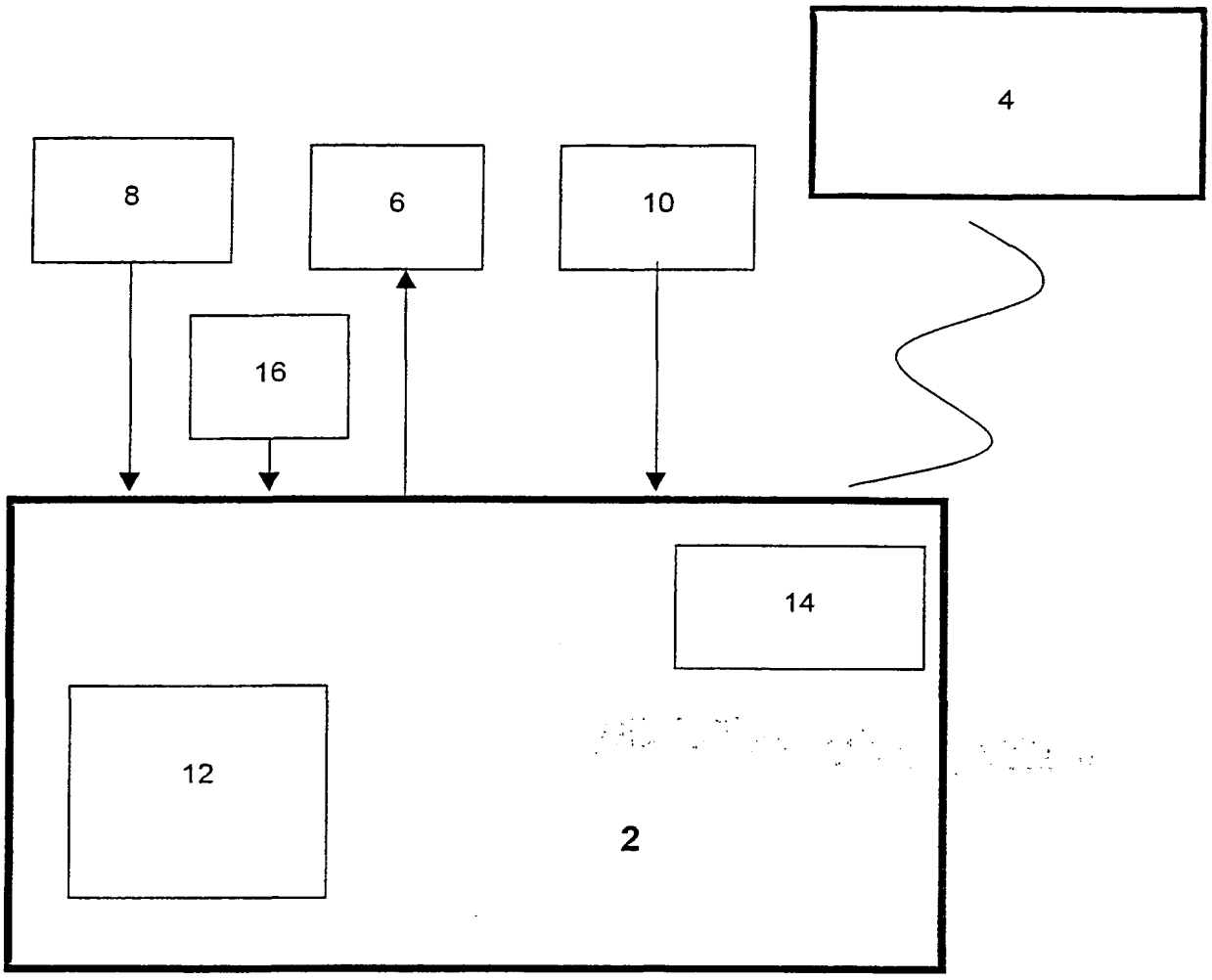
25. Ein Sicherheitssystem gemäß einem der Ansprüche 15 bis 24, in welchem die Befugnis Zugang zu dem gesicherten Gegenstand gewährt.

26. Ein Sicherheitssystem gemäß Anspruch 25, in welchem der gesicherte Gegenstand ein Fahrzeug ist.

27. Ein Sicherheitssystem gemäß einem der Ansprüche 15 bis 24, in welchem der gesicherte Gegenstand ein Fahrzeug ist und die Befugnis die Inbetriebnahme des Fahrzeugs gewährt.

28. Ein Sicherheitssystem gemäß Anspruch 27, in welchem die Inbetriebnahme das Starten des Fahrzeugs einschließt.

29. Ein Fahrzeug einschließlich eines Sicherheitssystems gemäß einem der Ansprüche 15 bis 28.



Figur 1